Exhibit 12

CHART FOR U.S. PATENT NO. 7,302,708 ("the '708 Patent")

Accused Products: VMWare's products, including at least each of the following security appliances and software infringe at least Claims 1: VMWare NSX. The infringement chart below is based on the VMWare NSX which is exemplary of the infringement of the '708 Patent.

Claims	Exemplary Infringement Evidence
[1pre] A method for secure access to a computer system, comprising the steps of:	To the extent the preamble is deemed limiting, the Accused Products perform a method for secure access to a computer system. For example, the VMWare NSX performs a method for secure access to a computer system. For example, the VMWare NSX performs the steps for malware prevention, intrusion detection and prevention, URL filtering and malware detection. These constitute a method for secure access to the computer system.

VMware NSX

VMware NSX® is the network virtualization and security platform that enables VMware's cloud networking solution with a software-defined approach to networking that extends across data centers, clouds and application frameworks. With NSX, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to physical servers. Like the operational model of VMs, networks can be provisioned and managed independent of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multitier networks—to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of the services offered via NSX or from a broad ecosystem of third-party integrations—ranging from next-generation firewalls to performance management solutions—to build inherently more agile and secure environments. These services can then be extended to a variety of endpoints within and across clouds.

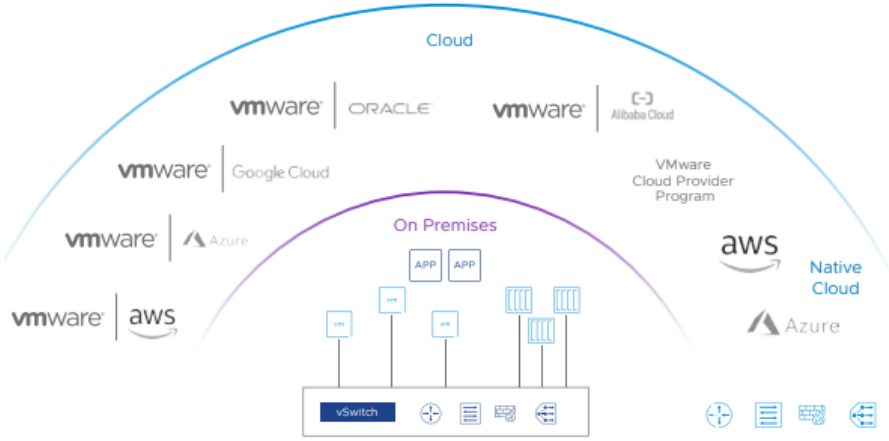


Figure 1: The NSX network virtualization and security platform.

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf

NSX distributed and gateway advanced security capabilities[2]	Several advanced security capabilities are available for NSX with security add-ons. These include: • Distributed security: – Distributed intrusion detection and prevention systems (IDPS) – Distributed malware prevention – Distributed network traffic analysis (NTA) – Network detection and response • Gateway security – URL filtering based on web categories and reputation • Malware detection

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf

As a further example, the VMWare NSX gateway firewall is a layer 2-7 firewall that achieves consistent network security coverage.

	At a glance VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that enables you to achieve consistent network security coverage and unified management for all of your workloads, regardless of whether they're running on physical servers, in a private or public cloud environment or in containers. When deployed together with the NSX Distributed Firewall, the Gateway Firewall extends its capabilities to deliver consistent protection across the entirety of the infrastructure. *See, e.g.*, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf As a further example, the VMWare NSX distributed firewall is a layer 7 firewall that delivers security with policy automation.

Operationalizing east-west security at scale

The VMware NSX Distributed Firewall is a software-defined Layer 7 firewall purpose-built to secure multi-cloud traffic across virtualized workloads. It provides stateful firewalling with IDS/IPS, sandboxing, and NTA/NDR—delivered as software and distributed to each host. With complete visibility into applications and flows, the NSX Distributed Firewall delivers superior security with policy automation that's linked to the workload lifecycle. Unlike traditional firewalls that require network redesign and traffic hair-pinning, the NSX Distributed Firewall distributes the firewalling to each host, radically simplifying the security architecture. This allows security teams to easily segment the network, stop the lateral movement of attacks, and automate policy in a vastly simpler operational model.

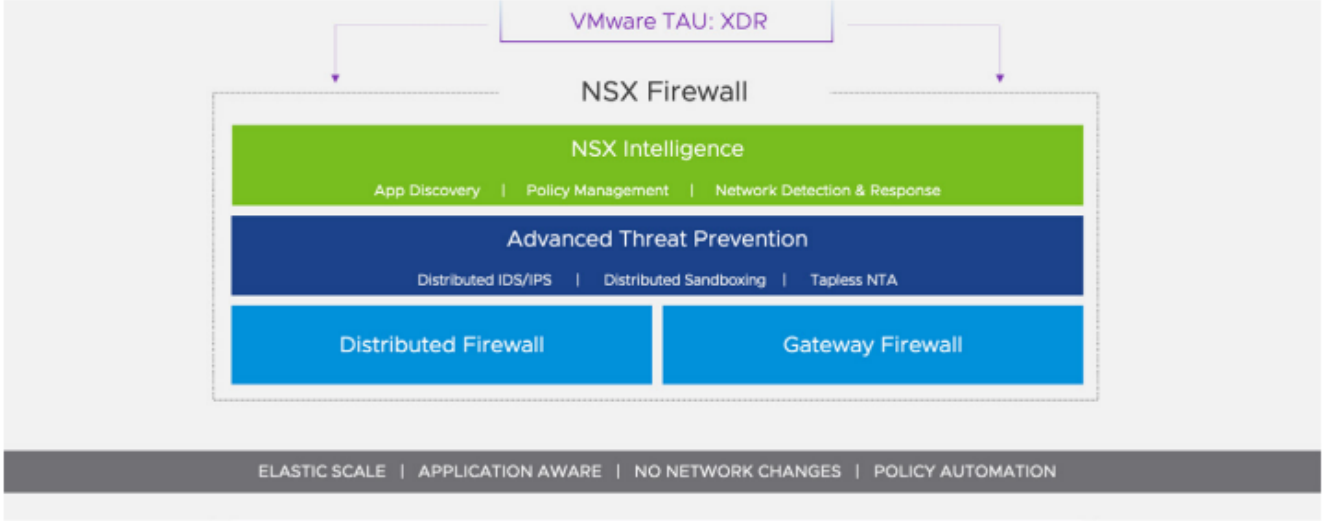


Figure 1: VMware NSX Distributed Firewall Architecture

	See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-distributed-firewall.pdf
[1a] receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;	The Accused Products receive in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function. For example, the VMWare NSX receives in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function. For example, the VMWare NSX performs intrusion detection and prevention, URL filtering and malware detection. It also enforces layer 2-7 access policies including application identity and user identity-based controls and network address translation. For example, any traffic in or out of a computing system is a request from an entity with a predetermined access level to a first base node.

A firewall to meet today's needs

VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection (using network sandboxing and other techniques) as well as routing and virtual private networking (VPN) functionality.

Key capabilities

Networking capabilities
The NSX Gateway Firewall provides a full suite of static and dynamic routing capabilities including IPv4 and IPv6, DNS, DHCP and comprehensive IP address management (IPAM).

Secure connectivity services
With support for layer 2 and 3 VPN services, the NSX Gateway Firewall enables secure low-latency connectivity across geographically diverse sites.

Access control
The NSX Gateway Firewall supports consistent enforcement of layer 2-7 access policies including application identity and user identity-based controls, URL filtering and network address translation (NAT).

Features	NSX Gateway Firewall	NSX Gateway Firewall with threat prevention	NSX Gateway Firewall with advanced threat prevention
L2-L4 access control	X	X	X
Static, dynamic routing	X	X	X
L2 and L3 VPNs	X	X	X
User identity-based access control	X	X	X
Application identity-based access control	X	X	X
URL filtering	X	X	X
TLS decryption	X	X	X
IDS/IPS		X	X
Network sandboxing			X

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf

[1b] determining if said access request completes a prohibited temporal access pattern for said entity;	The Accused Products determine if said access request completes a prohibited temporal access pattern for said entity. For example, the VMWare NSX determines if said access request completes a prohibited temporal access pattern for said entity. For example, any network traffic requesting access to a computing system is a request in which the NSX determines if it completes a prohibited temporal access pattern. It does this by employing the Advanced Thread Prevention (ATP) feature. This feature performs Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis. IDS/IPS looks for known malicious traffic patterns which constitute a temporal access pattern. Further, the Network Traffic Analysis uses machine learning and advanced statistical techniques to generate a temporal access pattern. VMware NSX Advanced Threat Prevention At a glance VMware's NSX Advanced Threat Prevention (ATP) provides network security capabilities that protect organizations against advanced threats. NSX ATP combines multiple detection technologies – Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis (NTA) – with aggregation, correlation, and context engines from Network Detection and Response (NDR). These capabilities complement each other to provide a cohesive defensive layer. As a result, ATP increases detection fidelity, reduces false positives, and accelerates remediation while decreasing security analysts' manual work.

Key capabilities

IDS/IPS

This technology inspects all traffic that enters or leaves the network, detecting and preventing known threats from gaining access to the network, critical systems, and data. IDS/IPS looks for known malicious traffic patterns to hunt for attacks in the traffic flow. When it finds such attacks, it generates alerts for use by security analysts. Alerts are also logged for post-incident investigation.

NTA

This technology looks at network traffic and traffic flow records using machine learning (ML) algorithms and advanced statistical techniques to develop a baseline of everyday activities. NTA can identify protocol, traffic, and host anomalies as they appear. Of course, not all anomalies represent threats; that's why VMware's NTA implements additional ML and rule-based techniques to determine if the anomaly is malicious. This analysis pipeline keeps false positives to a minimum, reducing the security team's work so the team can focus on real issues.

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-advanced-threat-prevention-ds.pdf

A firewall to meet today's needs

VMware NSX Gateway Firewall is a software-only, layer 2-7 firewall that incorporates advanced threat prevention capabilities such as intrusion detection/prevention (IDS/IPS), URL filtering and malware detection (using network sandboxing and other techniques) as well as routing and virtual private networking (VPN) functionality.

Key capabilities

Networking capabilities
The NSX Gateway Firewall provides a full suite of static and dynamic routing capabilities including IPv4 and IPv6, DNS, DHCP and comprehensive IP address management (IPAM).

Secure connectivity services
With support for layer 2 and 3 VPN services, the NSX Gateway Firewall enables secure low-latency connectivity across geographically diverse sites.

Access control
The NSX Gateway Firewall supports consistent enforcement of layer 2-7 access policies including application identity and user identity-based controls, URL filtering and network address translation (NAT).

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf

Key features	
Context-aware micro-segmentation	Security groups and policies can be dynamically created and automatically updated based on attributes—beyond just IP addresses, ports and protocols—to include elements such as machine name and tags, operating system type and Layer 7 application information to enable adaptive micro-segmentation policy. Policies based on identity information from Active Directory and other sources enable user-level security down to the individual user session level in remote desktop services and virtual desktop infrastructure (VDI) environments.
VMware NSX Intelligence™	Get automated security policy recommendations and continuous monitoring and visualization of every network traffic flow for enhanced visibility, enabling a highly and easily auditable security posture. As part of the same UI as VMware NSX, NSX Intelligence provides a single pane of glass for network and security teams.

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf

For example, this includes malicious IP address filtering, Signature based IDS/IPS and behavior based IDS.

	NSX Distributed Firewall	NSX Distributed Firewall with Threat Prevention	NSX Distributed Firewall with Advanced Threat Prevention
L2 – L4 firewalling	X	X	X
L7 Application Identity based firewalling	X	X	X
User Identity based firewalling	X	X	X
NSX Intelligence (flow visualization, policy recommendation)	X	X	X
Malicious IP address filtering	X	X	X
vRealize Log Insight	X	X	X
Signature based IDS/IPS		X	X
Behavior based IDS		X	X
NTA			X
Network Sandbox			X
NDR			X

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-distributed-firewall.pdf

	This is further described in the NSX Reference Design Guide:

5 NSX Security

In addition to providing network virtualization, NSX also serves as an advanced security platform, providing a rich set of features to streamline the deployment of security solutions. This chapter focuses on core NSX security capabilities, architecture, components, and implementation. Key concepts for examination include:

- NSX distributed firewall (DFW) provides stateful protection of the workload at the vNIC level. For ESXi, the DFW enforcement occurs in the hypervisor kernel, helping deliver micro-segmentation. However, the DFW extends to physical servers, KVM hypervisors, containers, and public clouds providing distributed policy enforcement.
- Uniform security policy model for on-premises and cloud deployment, supporting multi-hypervisor (i.e., ESXi and KVM) and multi-workload, with a level of granularity down to VM/containers/bare metal attributes.
- Agnostic to compute domain - supporting hypervisors managed by different compute-managers while allowing any defined micro-segmentation policy to be applied across hypervisors spanning multiple vCenter environments.
- Support for Layer 3, Layer 4, Layer-7 APP-ID, & Identity based firewall policies provide security via protocol, port, and or deeper packet/session intelligence to suit diverse needs.
- NSX Gateway firewall serves as a centralized stateful firewall service for N-S traffic. Gateway firewall is implemented per gateway and supported at both Tier-0 and Tier-1. Gateway firewall is independent of NSX DFW from policy configuration and enforcement perspective, providing a means for defining perimeter security control in addition to distributed security control.
- Gateway & Distributed Firewall Service insertion capability to integrate existing security investments using integration with partner ecosystem products on a granular basis without the need for interrupting natural traffic flows.
- Distributed IDS extends IDS capabilities to every host in the environment.
- Dynamic grouping of objects into logical constructs called Groups based on various criteria including tag, virtual machine name or operating system, subnet, and segments which automates policy application.
- The scope of policy enforcement can be selective, with application or workload-level granularity.
- Firewall Flood Protection capability to protect the workload & hypervisor resources.
- IP discovery mechanism dynamically identifies workload addressing.
- SpoofGuard blocks IP spoofing at vNIC level.

- Switch Security provides storm control and security against unauthorized traffic.

NSX 3.2 introduces advanced security features such as security on vCenter dvpgs, distributed and centralized malware protection, centralized IDS/IPS, URL Filtering, extensive next generation firewall App Identification support, Network Traffic Anomaly Detection, and Network Detection and Response (NDR). These new features will be covered in the new version if the SECURITY DESIGN GUIDE. This document will cover the NSX core security feature.

5.5 Intrusion Detection

Much like distributed firewalling changed the game on firewalling by providing a distributed, ubiquitous enforcement plane, NSX distributed IPS/IPS changes the game on IPS by providing a distributed, ubiquitous enforcement plane. However, there are additional benefits that the NSX distributed IPS model brings beyond ubiquity (which in itself is a game changer). NSX IPS is IPS distributed across all the hosts. Much like with DFW, the distributed nature allows the IPS

	capacity to grow linearly with compute capacity. Beyond that, however, there is an added benefit to distributing IPS. This is the added context. Legacy network Intrusion Detection and Prevention systems are deployed centrally in the network and rely either on traffic to be hairpinned through them or a copy of the traffic to be sent to them via techniques like SPAN or TAPs. These sensors typically match all traffic against all or a broad set of signatures and have very little context about the assets they are protecting. Applying all signatures to all traffic is very inefficient, as IDS/IPS unlike firewalling needs to look at the packet payload, not just the network headers. Each signature that needs to be matched against the traffic adds inspection overhead and potential latency introduced. Also, because legacy network IDS/IPS appliances just see packets without having context about the protected workloads, it's very difficult for security teams to determine the appropriate priority for each incident. Obviously, a successful intrusion against a vulnerable database server in production which holds mission-critical data needs more attention than someone in the IT staff triggering an IDS event by running a vulnerability scan. Because the NSX distributed IDS/IPS is applied to the vNIC of every workload, traffic does not need to hairpinned to a centralized appliance, and we can be very selective as to what signatures are applied. Signatures related to a windows vulnerability don't need to be applied to Linux workloads, or servers running Apache don't need signatures that detect an exploit of a database service. Through the Guest Introspection Framework, and in-guest drivers, NSX has access to context about each guest, including the operating system version, users logged in or any running process. This context can be leveraged to selectively apply only the relevant signatures, not only reducing the processing impact, but more importantly reducing the noise and quantity of false positives compared to what would be seen if all signatures are applied to all traffic with a traditional appliance. For a detailed description of IDS configuration, see the NSX Product Documentation.

5.7 Additional Security Features

NSX extends the security solution beyond DFW with additional features to enhance data center security posture on top of micro-segmentation. These features include:

- **SpoofGuard** - Provides protection against spoofing with MAC+IP+VLAN bindings. This can be enforced at a per logical port level. The SpoofGuard feature requires static or dynamic bindings (e.g., DHCP/ARP snooping) of IP+MAC for enforcement.
- **Segment Security** - Provides stateless L2 and L3 security to protect segment integrity by filtering out malicious attacks (e.g., denial of service using broadcast/multicast storms) and unauthorized traffic entering segment from VMs. This is accomplished by attaching the segment security profile to a segment for enforcement. The segment security profile has options to allow/block bridge protocol data unit (BPDU), DHCP server/client traffic, non-IP traffic. It allows for rate limiting of broadcast and multicast traffic, both transmitted and received.

See, e.g., https://communities.vmware.com/t5/VMware-NSX-Documents/VMware-NSX-T-Reference-Design/ta-p/2778093

Virtual Firewalling is described further in the Security Reference Guide:

5.1 Rule Lookup

NSX firewalls implement a top down rule search order. When a packet matches, it pops out of the search bas processing indicated in the matched rule.

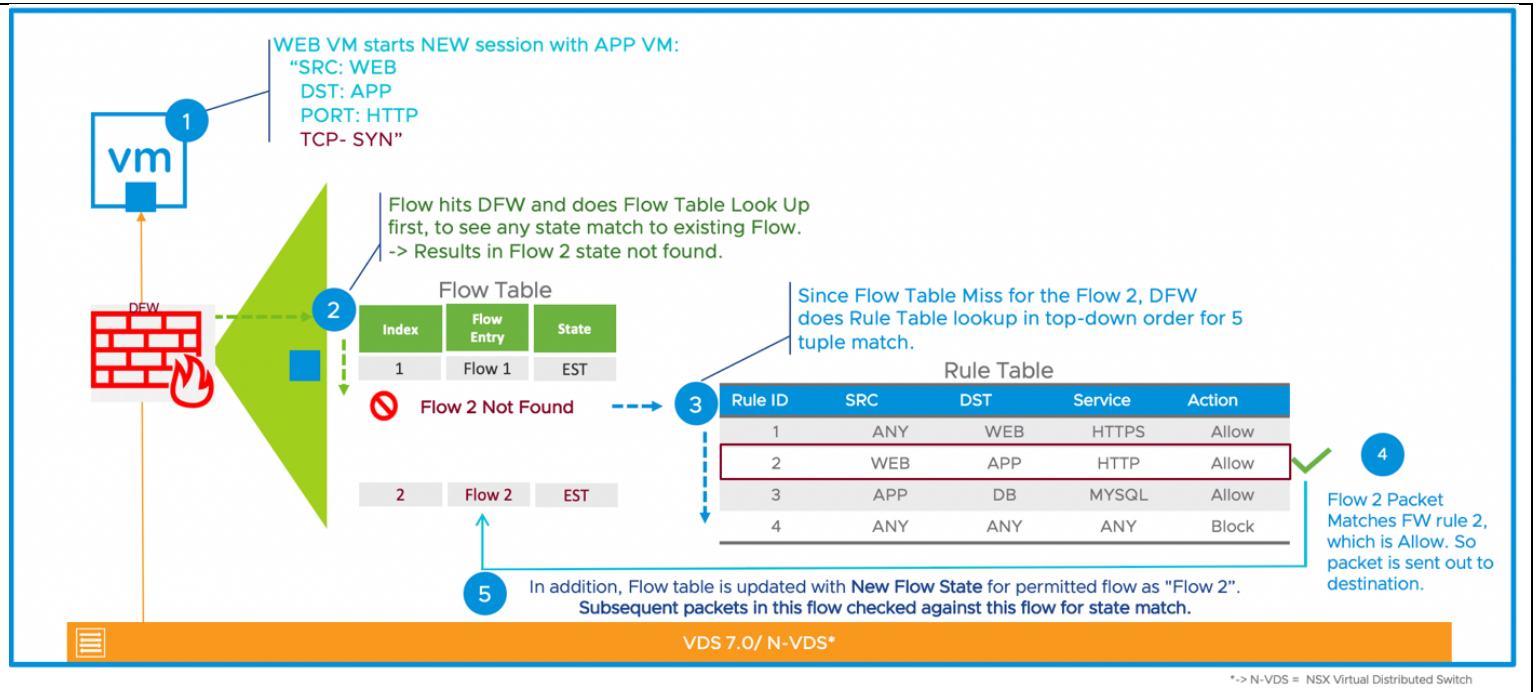
By default, the DFW implements the rule table and flow table model that most firewalls use. However, this bel overwritten for troubleshooting or other corner cases as described later.

In figure 4.1, the processing of a packet takes place as follows:
An IP packet identified as pkt1 that matches rule number 2. The order of operation is the following:

1. A lookup is performed in the connection tracker table to determine if an entry for the flow already exist
2. As flow 3 is not present in the connection tracker table, a lookup is performed in the rule table to identif is applicable to flow 3. The first rule that matches the flow will be enforced.
3. Rule 2 matches for flow 3. The action is set to 'Allow'.
4. Because the action is set to 'Allow' for flow 3, a new entry will be created inside the connection tracker packet is then transmitted out of DFW.

Subsequent packets are processed in this order:

1. A lookup is performed in the connection tracker table to check if an entry for the flow already exists.
2. An entry for flow 3 exists in the connection tracker table. The packet is transmitted out of DFW



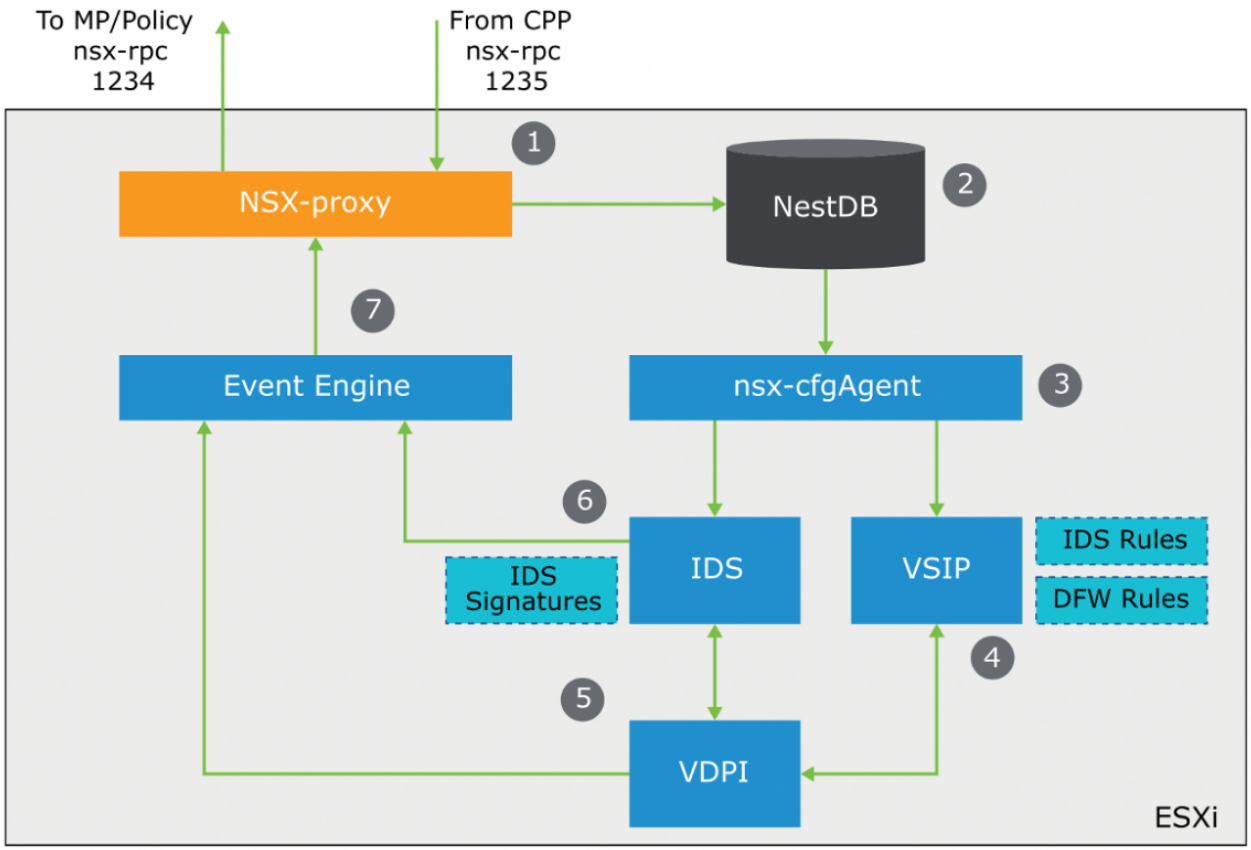
See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-51--rule-lookup

IPS is described further in the Security Reference Guide:

8.1 NSX IPS Components

The NSX IPS components are the same as those described above for DFW as IPS functionality is collocated with DFW. In the Management plane, the Manager downloads IPS signature updates from the cloud service and users configure IPS profiles and rules. As with the DFW, the configuration is passed to the CCP after being stored in the Manager. Again, as with DFW, the CCP pushes the information to the LCP on the hosts. At the host, the signature information is stored in a database on the host and configured in the datapath. The ESXi host also collects traffic data and events to pass up to the NSX manager.

Figure 8 - 2 NSX-T IPS Components – LCP and host below shows the detail of the IPS components inside the host.

	 *See, e.g.*, https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-81-nsx-ips-components
[1c] comparing a minimum access level established for said first base node to	The accused Products compare a minimum access level established for said first base node to said predetermined access level. For example, the VMWare NSX compares a minimum access level established for said first base node to said predetermined access level.

<table>
<tr>
<td>said predetermined access level;</td>
<td>For example, any network traffic requesting access to a computing system is a request in which the NSX determines if it completes a prohibited temporal access pattern. The NSX compares a minimum access level established to a predetermined access level. It does this by employing the Advanced Thread Prevention (ATP) feature. This feature performs Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis. IDS/IPS looks for known malicious traffic patterns which constitute a temporal access pattern. Further, the Network Traffic Analysis uses machine learning and advanced statistical techniques to generate a temporal access pattern.

<table>
<tr><th colspan="2">Key features</th></tr>
<tr><td>Context-aware micro-segmentation</td><td>Security groups and policies can be dynamically created and automatically updated based on attributes—beyond just IP addresses, ports and protocols—to include elements such as machine name and tags, operating system type and Layer 7 application information to enable adaptive micro-segmentation policy. Policies based on identity information from Active Directory and other sources enable user-level security down to the individual user session level in remote desktop services and virtual desktop infrastructure (VDI) environments.</td></tr>
<tr><td>VMware NSX Intelligence™</td><td>Get automated security policy recommendations and continuous monitoring and visualization of every network traffic flow for enhanced visibility, enabling a highly and easily auditable security posture. As part of the same UI as VMware NSX, NSX Intelligence provides a single pane of glass for network and security teams.</td></tr>
</table>

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf

For example, this includes malicious IP address filtering, Signature based IDS/IPS and behavior based IDS.</td>
</tr>
</table>

	NSX Distributed Firewall	NSX Distributed Firewall with Threat Prevention	NSX Distributed Firewall with Advanced Threat Prevention
L2 – L4 firewalling	X	X	X
L7 Application Identity based firewalling	X	X	X
User Identity based firewalling	X	X	X
NSX Intelligence (flow visualization, policy recommendation)	X	X	X
Malicious IP address filtering	X	X	X
vRealize Log Insight	X	X	X
Signature based IDS/IPS		X	X
Behavior based IDS		X	X
NTA			X
Network Sandbox			X
NDR			X

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-distributed-firewall.pdf

	This is further described in the NSX Reference Design Guide:

5 NSX Security

In addition to providing network virtualization, NSX also serves as an advanced security platform, providing a rich set of features to streamline the deployment of security solutions. This chapter focuses on core NSX security capabilities, architecture, components, and implementation. Key concepts for examination include:

- NSX distributed firewall (DFW) provides stateful protection of the workload at the vNIC level. For ESXi, the DFW enforcement occurs in the hypervisor kernel, helping deliver micro-segmentation. However, the DFW extends to physical servers, KVM hypervisors, containers, and public clouds providing distributed policy enforcement.
- Uniform security policy model for on-premises and cloud deployment, supporting multi-hypervisor (i.e., ESXi and KVM) and multi-workload, with a level of granularity down to VM/containers/bare metal attributes.
- Agnostic to compute domain - supporting hypervisors managed by different compute-managers while allowing any defined micro-segmentation policy to be applied across hypervisors spanning multiple vCenter environments.
- Support for Layer 3, Layer 4, Layer-7 APP-ID, & Identity based firewall policies provide security via protocol, port, and or deeper packet/session intelligence to suit diverse needs.
- NSX Gateway firewall serves as a centralized stateful firewall service for N-S traffic. Gateway firewall is implemented per gateway and supported at both Tier-0 and Tier-1. Gateway firewall is independent of NSX DFW from policy configuration and enforcement perspective, providing a means for defining perimeter security control in addition to distributed security control.
- Gateway & Distributed Firewall Service insertion capability to integrate existing security investments using integration with partner ecosystem products on a granular basis without the need for interrupting natural traffic flows.
- Distributed IDS extends IDS capabilities to every host in the environment.
- Dynamic grouping of objects into logical constructs called Groups based on various criteria including tag, virtual machine name or operating system, subnet, and segments which automates policy application.
- The scope of policy enforcement can be selective, with application or workload-level granularity.
- Firewall Flood Protection capability to protect the workload & hypervisor resources.
- IP discovery mechanism dynamically identifies workload addressing.
- SpoofGuard blocks IP spoofing at vNIC level.

- Switch Security provides storm control and security against unauthorized traffic.

NSX 3.2 introduces advanced security features such as security on vCenter dvpgs, distributed and centralized malware protection, centralized IDS/IPS, URL Filtering, extensive next generation firewall App Identification support, Network Traffic Anomaly Detection, and Network Detection and Response (NDR). These new features will be covered in the new version if the SECURITY DESIGN GUIDE. This document will cover the NSX core security feature.

5.5 Intrusion Detection

Much like distributed firewalling changed the game on firewalling by providing a distributed, ubiquitous enforcement plane, NSX distributed IPS/IPS changes the game on IPS by providing a distributed, ubiquitous enforcement plane. However, there are additional benefits that the NSX distributed IPS model brings beyond ubiquity (which in itself is a game changer). NSX IPS is IPS distributed across all the hosts. Much like with DFW, the distributed nature allows the IPS

	capacity to grow linearly with compute capacity. Beyond that, however, there is an added benefit to distributing IPS. This is the added context. Legacy network Intrusion Detection and Prevention systems are deployed centrally in the network and rely either on traffic to be hairpinned through them or a copy of the traffic to be sent to them via techniques like SPAN or TAPs. These sensors typically match all traffic against all or a broad set of signatures and have very little context about the assets they are protecting. Applying all signatures to all traffic is very inefficient, as IDS/IPS unlike firewalling needs to look at the packet payload, not just the network headers. Each signature that needs to be matched against the traffic adds inspection overhead and potential latency introduced. Also, because legacy network IDS/IPS appliances just see packets without having context about the protected workloads, it's very difficult for security teams to determine the appropriate priority for each incident. Obviously, a successful intrusion against a vulnerable database server in production which holds mission-critical data needs more attention than someone in the IT staff triggering an IDS event by running a vulnerability scan. Because the NSX distributed IDS/IPS is applied to the vNIC of every workload, traffic does not need to hairpinned to a centralized appliance, and we can be very selective as to what signatures are applied. Signatures related to a windows vulnerability don't need to be applied to Linux workloads, or servers running Apache don't need signatures that detect an exploit of a database service. Through the Guest Introspection Framework, and in-guest drivers, NSX has access to context about each guest, including the operating system version, users logged in or any running process. This context can be leveraged to selectively apply only the relevant signatures, not only reducing the processing impact, but more importantly reducing the noise and quantity of false positives compared to what would be seen if all signatures are applied to all traffic with a traditional appliance. For a detailed description of IDS configuration, see the NSX Product Documentation.

5.7 Additional Security Features

NSX extends the security solution beyond DFW with additional features to enhance data center security posture on top of micro-segmentation. These features include:

- **SpoofGuard** - Provides protection against spoofing with MAC+IP+VLAN bindings. This can be enforced at a per logical port level. The SpoofGuard feature requires static or dynamic bindings (e.g., DHCP/ARP snooping) of IP+MAC for enforcement.
- **Segment Security** - Provides stateless L2 and L3 security to protect segment integrity by filtering out malicious attacks (e.g., denial of service using broadcast/multicast storms) and unauthorized traffic entering segment from VMs. This is accomplished by attaching the segment security profile to a segment for enforcement. The segment security profile has options to allow/block bridge protocol data unit (BPDU), DHCP server/client traffic, non-IP traffic. It allows for rate limiting of broadcast and multicast traffic, both transmitted and received.

See, e.g., https://communities.vmware.com/t5/VMware-NSX-Documents/VMware-NSX-T-Reference-Design/ta-p/2778093

Virtual Firewalling is described further in the Security Reference Guide:

5.1 Rule Lookup

NSX firewalls implement a top down rule search order. When a packet matches, it pops out of the search bas processing indicated in the matched rule.

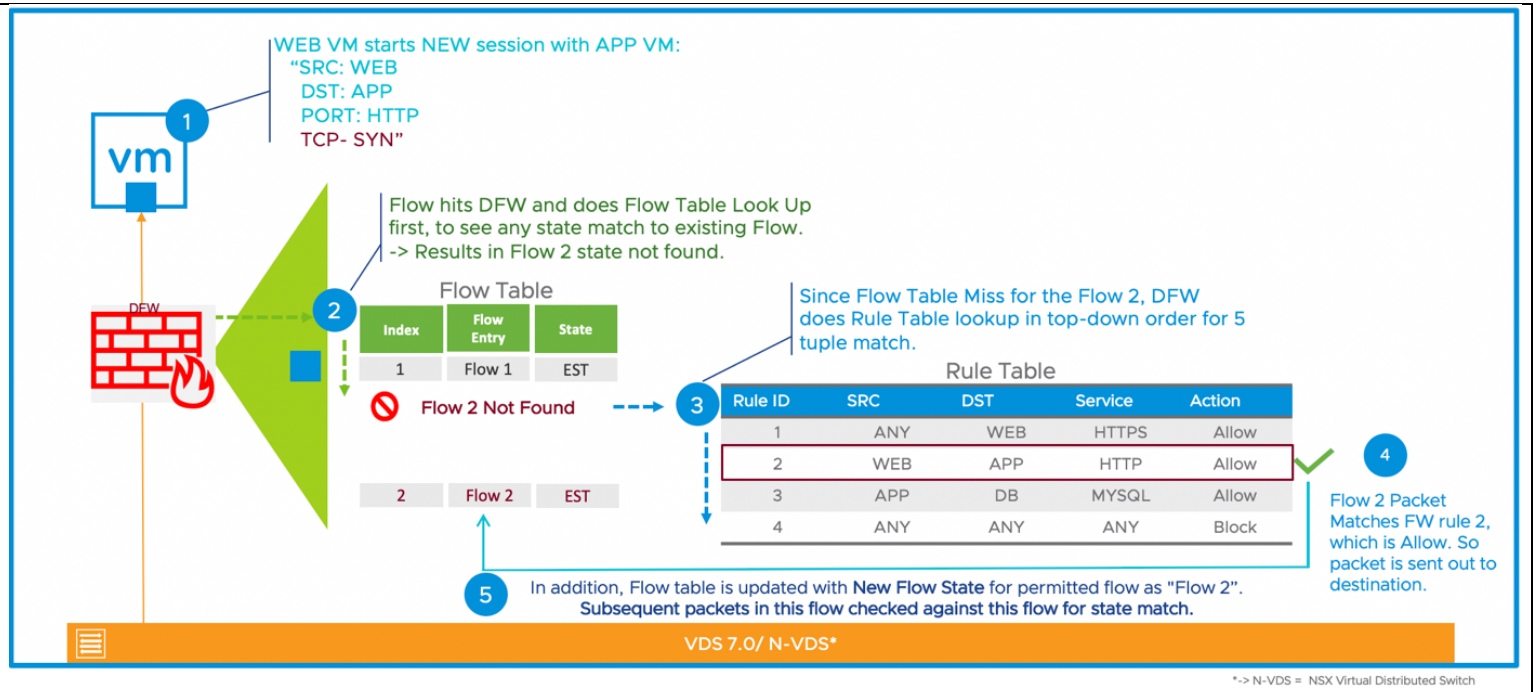
By default, the DFW implements the rule table and flow table model that most firewalls use. However, this bel overwritten for troubleshooting or other corner cases as described later.

In figure 4.1, the processing of a packet takes place as follows:
An IP packet identified as pkt1 that matches rule number 2. The order of operation is the following:

1. A lookup is performed in the connection tracker table to determine if an entry for the flow already exist
2. As flow 3 is not present in the connection tracker table, a lookup is performed in the rule table to identif is applicable to flow 3. The first rule that matches the flow will be enforced.
3. Rule 2 matches for flow 3. The action is set to 'Allow'.
4. Because the action is set to 'Allow' for flow 3, a new entry will be created inside the connection tracker packet is then transmitted out of DFW.

Subsequent packets are processed in this order:

1. A lookup is performed in the connection tracker table to check if an entry for the flow already exists.
2. An entry for flow 3 exists in the connection tracker table. The packet is transmitted out of DFW



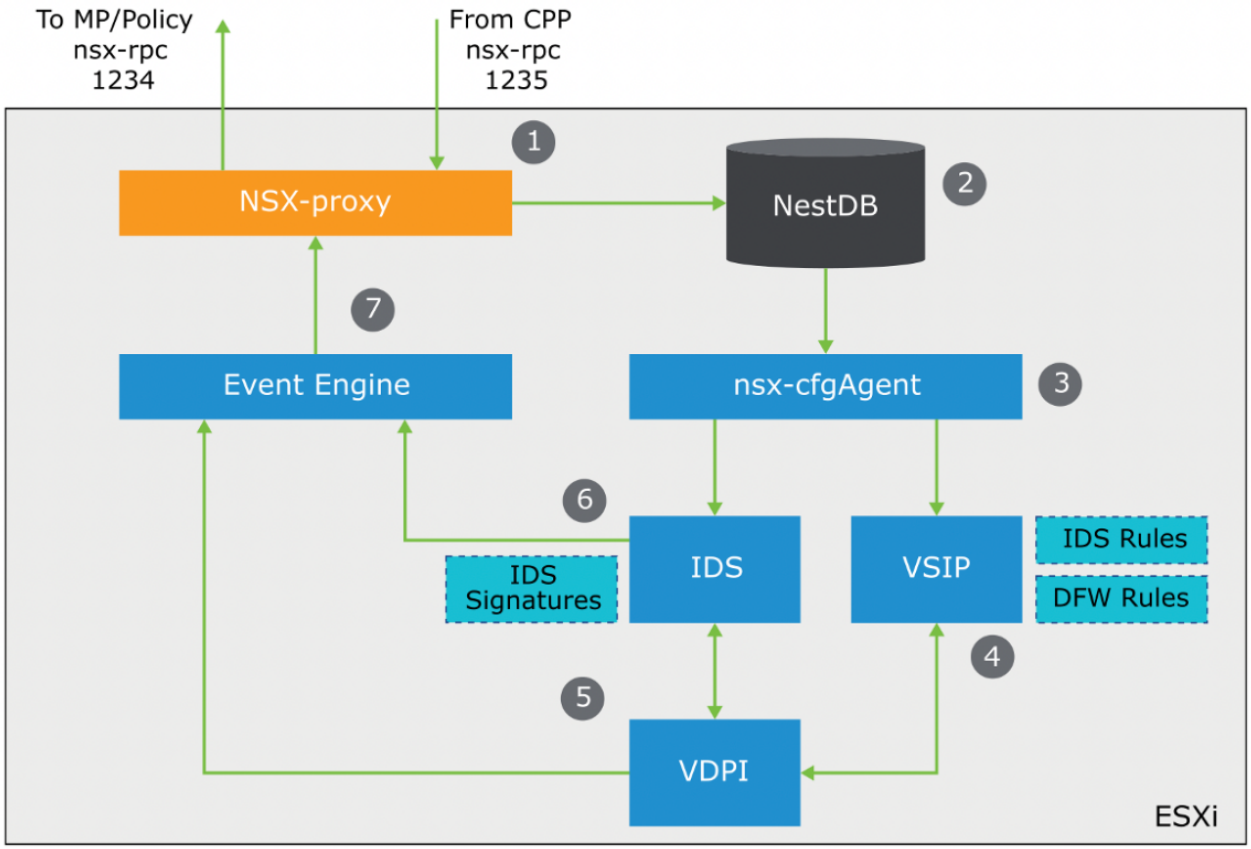
See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-51--rule-lookup

IPS is described further in the Security Reference Guide:

8.1 NSX IPS Components

The NSX IPS components are the same as those described above for DFW as IPS functionality is collocated with DFW. In the Management plane, the Manager downloads IPS signature updates from the cloud service and users configure IPS profiles and rules. As with the DFW, the configuration is passed to the CCP after being stored in the Manager. Again, as with DFW, the CCP pushes the information to the LCP on the hosts. At the host, the signature information is stored in a database on the host and configured in the datapath. The ESXi host also collects traffic data and events to pass up to the NSX manager.

Figure 8 - 2 NSX-T IPS Components – LCP and host below shows the detail of the IPS components inside the host.



See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-81-nsx-ips-components

Virtual Firewalling is described further in the Security Reference Guide:

5.1 Rule Lookup

NSX firewalls implement a top down rule search order. When a packet matches, it pops out of the search bas processing indicated in the matched rule.

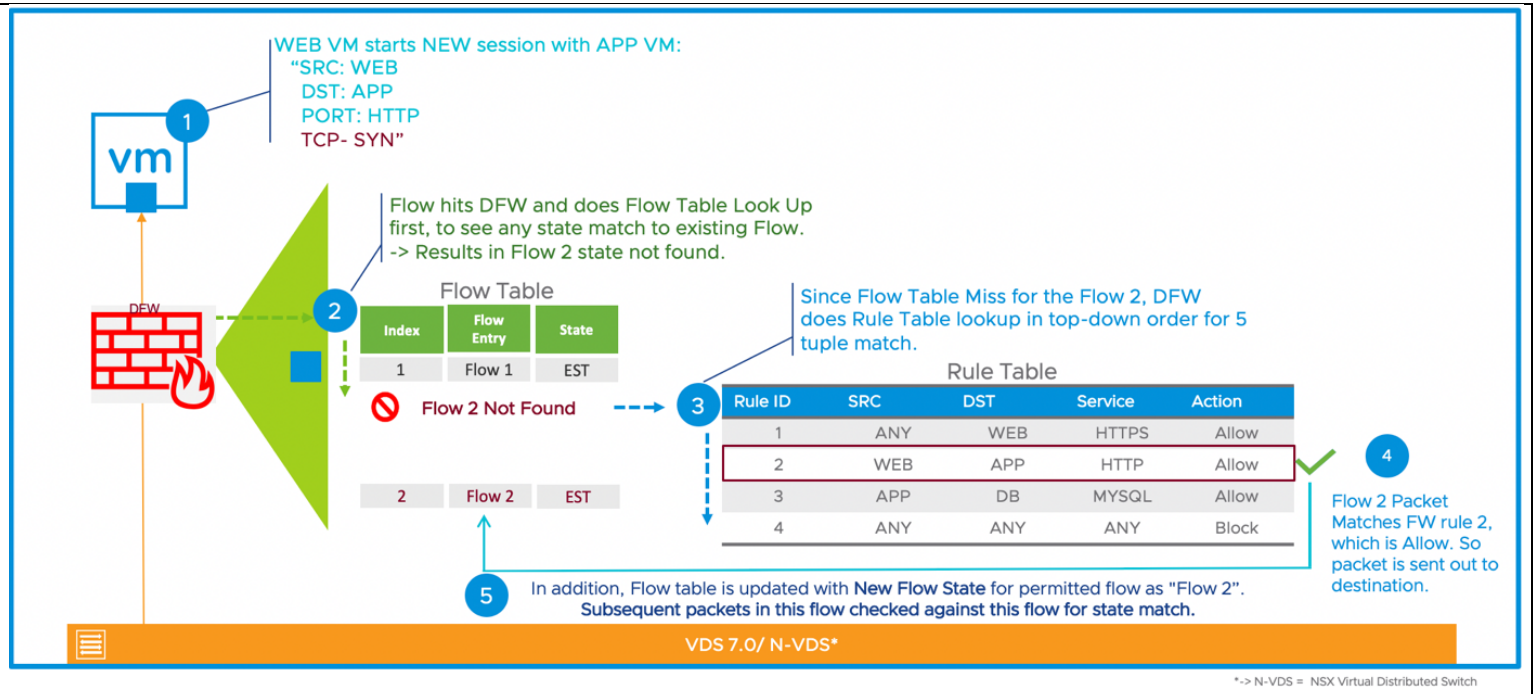
By default, the DFW implements the rule table and flow table model that most firewalls use. However, this bel overwritten for troubleshooting or other corner cases as described later.

In figure 4.1, the processing of a packet takes place as follows:
An IP packet identified as pkt1 that matches rule number 2. The order of operation is the following:

1. A lookup is performed in the connection tracker table to determine if an entry for the flow already exist
2. As flow 3 is not present in the connection tracker table, a lookup is performed in the rule table to identif is applicable to flow 3. The first rule that matches the flow will be enforced.
3. Rule 2 matches for flow 3. The action is set to 'Allow'.
4. Because the action is set to 'Allow' for flow 3, a new entry will be created inside the connection tracker packet is then transmitted out of DFW.

Subsequent packets are processed in this order:

1. A lookup is performed in the connection tracker table to check if an entry for the flow already exists.
2. An entry for flow 3 exists in the connection tracker table. The packet is transmitted out of DFW



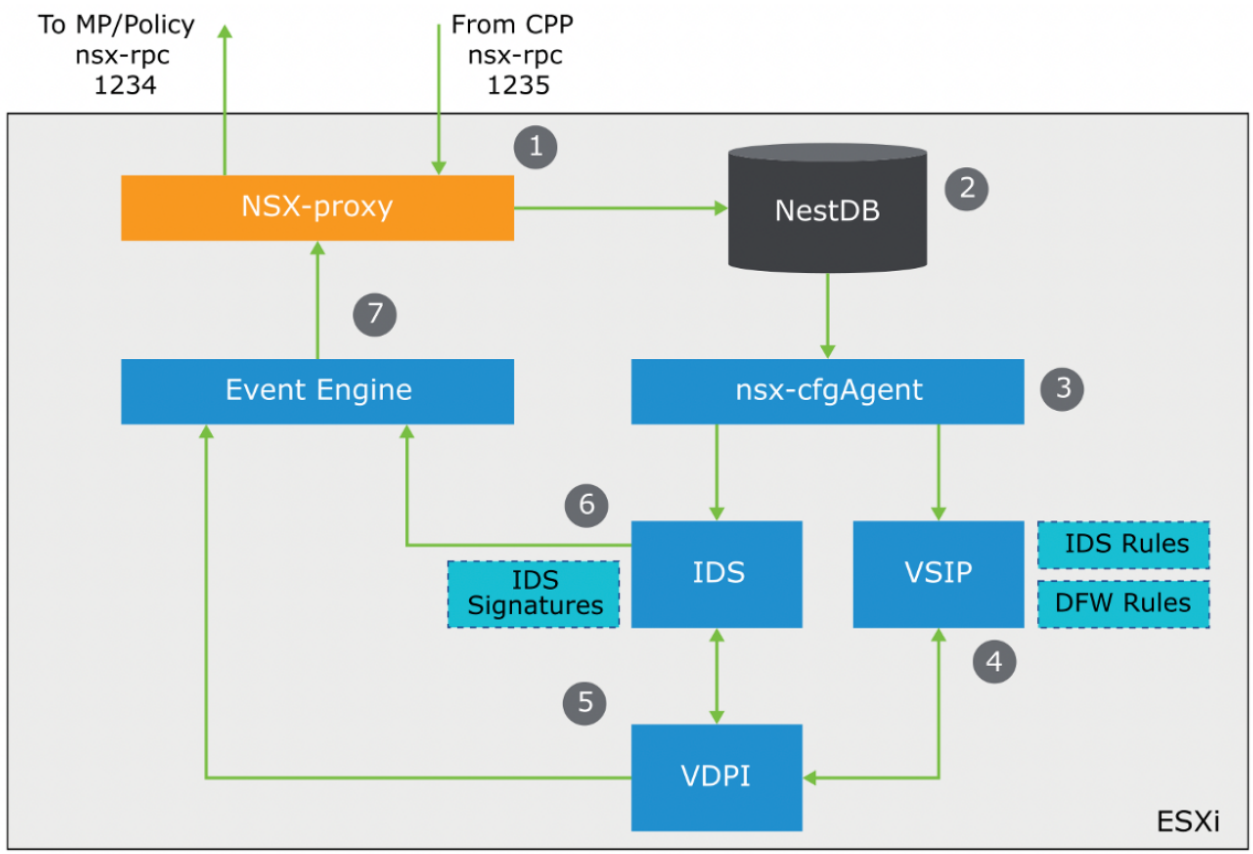
See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-51--rule-lookup

IPS is described further in the Security Reference Guide:

8.1 NSX IPS Components

The NSX IPS components are the same as those described above for DFW as IPS functionality is collocated with DFW. In the Management plane, the Manager downloads IPS signature updates from the cloud service and users configure IPS profiles and rules. As with the DFW, the configuration is passed to the CCP after being stored in the Manager. Again, as with DFW, the CCP pushes the information to the LCP on the hosts. At the host, the signature information is stored in a database on the host and configured in the datapath. The ESXi host also collects traffic data and events to pass up to the NSX manager.

Figure 8 - 2 NSX-T IPS Components – LCP and host below shows the detail of the IPS components inside the host.

	 *See, e.g.*, https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-81-nsx-ips-components
[1d] granting said access request only if it does not complete a	The Accused Products grant said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level. For example, the VMWare NSX grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and	For example, any network traffic requesting access to a computing system is a request in which the NSX determines if it completes a prohibited temporal access pattern. The NSX compares a minimum access level established to a predetermined access level. The request is granted only if it does not complete a prohibited temporal access pattern. It does this by employing the Advanced Thread Prevention (ATP) feature. This feature performs Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis. IDS/IPS looks for known malicious traffic patterns which constitute a temporal access pattern. Further, the Network Traffic Analysis uses machine learning and advanced statistical techniques to generate a temporal access pattern. VMware NSX Advanced Threat Prevention At a glance VMware's NSX Advanced Threat Prevention (ATP) provides network security capabilities that protect organizations against advanced threats. NSX ATP combines multiple detection technologies – Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis (NTA) – with aggregation, correlation, and context engines from Network Detection and Response (NDR). These capabilities complement each other to provide a cohesive defensive layer. As a result, ATP increases detection fidelity, reduces false positives, and accelerates remediation while decreasing security analysts' manual work.

Key capabilities

IDS/IPS

This technology inspects all traffic that enters or leaves the network, detecting and preventing known threats from gaining access to the network, critical systems, and data. IDS/IPS looks for known malicious traffic patterns to hunt for attacks in the traffic flow. When it finds such attacks, it generates alerts for use by security analysts. Alerts are also logged for post-incident investigation.

NTA

This technology looks at network traffic and traffic flow records using machine learning (ML) algorithms and advanced statistical techniques to develop a baseline of everyday activities. NTA can identify protocol, traffic, and host anomalies as they appear. Of course, not all anomalies represent threats; that's why VMware's NTA implements additional ML and rule-based techniques to determine if the anomaly is malicious. This analysis pipeline keeps false positives to a minimum, reducing the security team's work so the team can focus on real issues.

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-advanced-threat-prevention-ds.pdf

Key features	
Context-aware micro-segmentation	Security groups and policies can be dynamically created and automatically updated based on attributes—beyond just IP addresses, ports and protocols—to include elements such as machine name and tags, operating system type and Layer 7 application information to enable adaptive micro-segmentation policy. Policies based on identity information from Active Directory and other sources enable user-level security down to the individual user session level in remote desktop services and virtual desktop infrastructure (VDI) environments.
VMware NSX Intelligence™	Get automated security policy recommendations and continuous monitoring and visualization of every network traffic flow for enhanced visibility, enabling a highly and easily auditable security posture. As part of the same UI as VMware NSX, NSX Intelligence provides a single pane of glass for network and security teams.

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf

For example, this includes malicious IP address filtering, Signature based IDS/IPS and behavior based IDS.

	NSX Distributed Firewall	NSX Distributed Firewall with Threat Prevention	NSX Distributed Firewall with Advanced Threat Prevention
L2 – L4 firewalling	X	X	X
L7 Application Identity based firewalling	X	X	X
User Identity based firewalling	X	X	X
NSX Intelligence (flow visualization, policy recommendation)	X	X	X
Malicious IP address filtering	X	X	X
vRealize Log Insight	X	X	X
Signature based IDS/IPS		X	X
Behavior based IDS		X	X
NTA			X
Network Sandbox			X
NDR			X

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-distributed-firewall.pdf

	This is further described in the NSX Reference Design Guide:

5 NSX Security

In addition to providing network virtualization, NSX also serves as an advanced security platform, providing a rich set of features to streamline the deployment of security solutions. This chapter focuses on core NSX security capabilities, architecture, components, and implementation. Key concepts for examination include:

- NSX distributed firewall (DFW) provides stateful protection of the workload at the vNIC level. For ESXi, the DFW enforcement occurs in the hypervisor kernel, helping deliver micro-segmentation. However, the DFW extends to physical servers, KVM hypervisors, containers, and public clouds providing distributed policy enforcement.
- Uniform security policy model for on-premises and cloud deployment, supporting multi-hypervisor (i.e., ESXi and KVM) and multi-workload, with a level of granularity down to VM/containers/bare metal attributes.
- Agnostic to compute domain - supporting hypervisors managed by different compute-managers while allowing any defined micro-segmentation policy to be applied across hypervisors spanning multiple vCenter environments.
- Support for Layer 3, Layer 4, Layer-7 APP-ID, & Identity based firewall policies provide security via protocol, port, and or deeper packet/session intelligence to suit diverse needs.
- NSX Gateway firewall serves as a centralized stateful firewall service for N-S traffic. Gateway firewall is implemented per gateway and supported at both Tier-0 and Tier-1. Gateway firewall is independent of NSX DFW from policy configuration and enforcement perspective, providing a means for defining perimeter security control in addition to distributed security control.
- Gateway & Distributed Firewall Service insertion capability to integrate existing security investments using integration with partner ecosystem products on a granular basis without the need for interrupting natural traffic flows.
- Distributed IDS extends IDS capabilities to every host in the environment.
- Dynamic grouping of objects into logical constructs called Groups based on various criteria including tag, virtual machine name or operating system, subnet, and segments which automates policy application.
- The scope of policy enforcement can be selective, with application or workload-level granularity.
- Firewall Flood Protection capability to protect the workload & hypervisor resources.
- IP discovery mechanism dynamically identifies workload addressing.
- SpoofGuard blocks IP spoofing at vNIC level.

- Switch Security provides storm control and security against unauthorized traffic.

NSX 3.2 introduces advanced security features such as security on vCenter dvpgs, distributed and centralized malware protection, centralized IDS/IPS, URL Filtering, extensive next generation firewall App Identification support, Network Traffic Anomaly Detection, and Network Detection and Response (NDR). These new features will be covered in the new version if the SECURITY DESIGN GUIDE. This document will cover the NSX core security feature.

5.5 Intrusion Detection

Much like distributed firewalling changed the game on firewalling by providing a distributed, ubiquitous enforcement plane, NSX distributed IPS/IPS changes the game on IPS by providing a distributed, ubiquitous enforcement plane. However, there are additional benefits that the NSX distributed IPS model brings beyond ubiquity (which in itself is a game changer). NSX IPS is IPS distributed across all the hosts. Much like with DFW, the distributed nature allows the IPS

	capacity to grow linearly with compute capacity. Beyond that, however, there is an added benefit to distributing IPS. This is the added context. Legacy network Intrusion Detection and Prevention systems are deployed centrally in the network and rely either on traffic to be hairpinned through them or a copy of the traffic to be sent to them via techniques like SPAN or TAPs. These sensors typically match all traffic against all or a broad set of signatures and have very little context about the assets they are protecting. Applying all signatures to all traffic is very inefficient, as IDS/IPS unlike firewalling needs to look at the packet payload, not just the network headers. Each signature that needs to be matched against the traffic adds inspection overhead and potential latency introduced. Also, because legacy network IDS/IPS appliances just see packets without having context about the protected workloads, it's very difficult for security teams to determine the appropriate priority for each incident. Obviously, a successful intrusion against a vulnerable database server in production which holds mission-critical data needs more attention than someone in the IT staff triggering an IDS event by running a vulnerability scan. Because the NSX distributed IDS/IPS is applied to the vNIC of every workload, traffic does not need to hairpinned to a centralized appliance, and we can be very selective as to what signatures are applied. Signatures related to a windows vulnerability don't need to be applied to Linux workloads, or servers running Apache don't need signatures that detect an exploit of a database service. Through the Guest Introspection Framework, and in-guest drivers, NSX has access to context about each guest, including the operating system version, users logged in or any running process. This context can be leveraged to selectively apply only the relevant signatures, not only reducing the processing impact, but more importantly reducing the noise and quantity of false positives compared to what would be seen if all signatures are applied to all traffic with a traditional appliance. For a detailed description of IDS configuration, see the NSX Product Documentation.

5.7 Additional Security Features

NSX extends the security solution beyond DFW with additional features to enhance data center security posture on top of micro-segmentation. These features include:

- **SpoofGuard** - Provides protection against spoofing with MAC+IP+VLAN bindings. This can be enforced at a per logical port level. The SpoofGuard feature requires static or dynamic bindings (e.g., DHCP/ARP snooping) of IP+MAC for enforcement.
- **Segment Security** - Provides stateless L2 and L3 security to protect segment integrity by filtering out malicious attacks (e.g., denial of service using broadcast/multicast storms) and unauthorized traffic entering segment from VMs. This is accomplished by attaching the segment security profile to a segment for enforcement. The segment security profile has options to allow/block bridge protocol data unit (BPDU), DHCP server/client traffic, non-IP traffic. It allows for rate limiting of broadcast and multicast traffic, both transmitted and received.

See, e.g., https://communities.vmware.com/t5/VMware-NSX-Documents/VMware-NSX-T-Reference-Design/ta-p/2778093

Virtual Firewalling is described further in the Security Reference Guide:

5.1 Rule Lookup

NSX firewalls implement a top down rule search order. When a packet matches, it pops out of the search bas processing indicated in the matched rule.

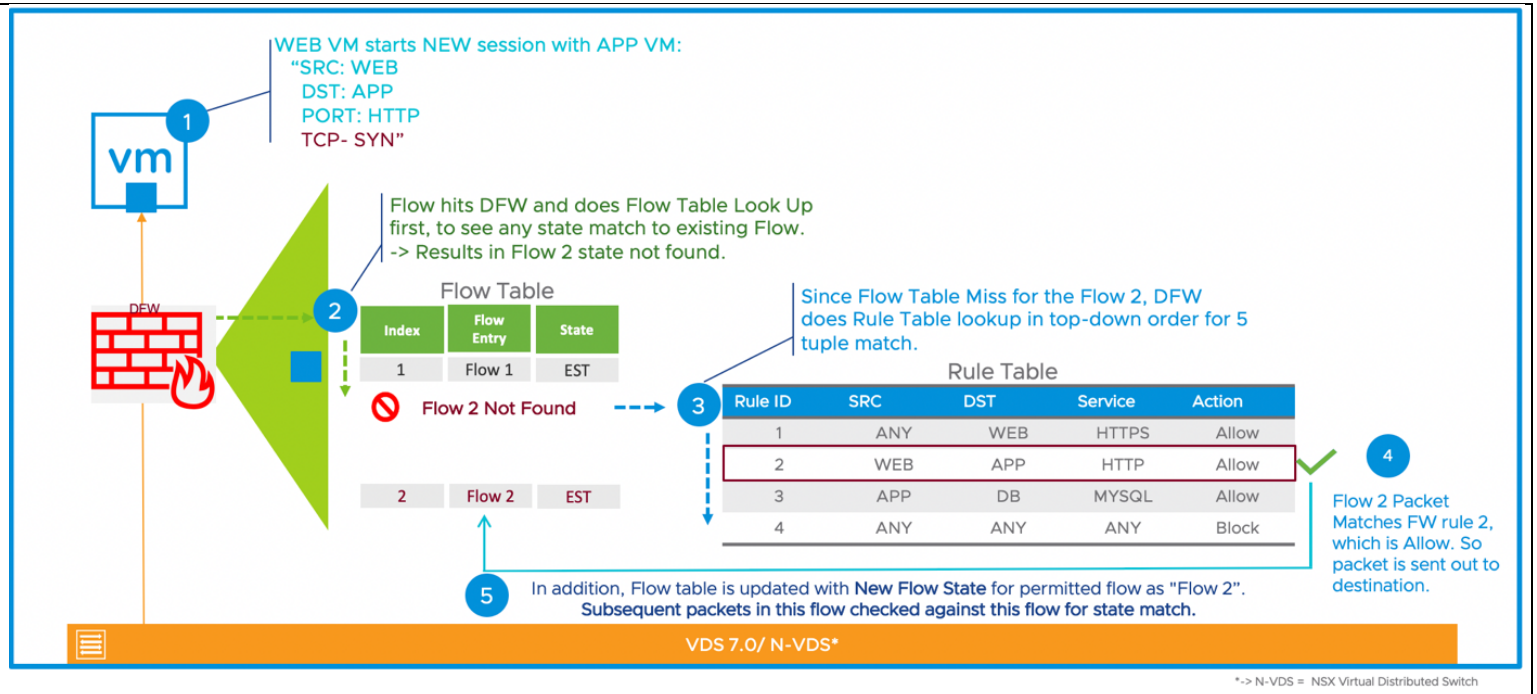
By default, the DFW implements the rule table and flow table model that most firewalls use. However, this bel overwritten for troubleshooting or other corner cases as described later.

In figure 4.1, the processing of a packet takes place as follows:
An IP packet identified as pkt1 that matches rule number 2. The order of operation is the following:

1. A lookup is performed in the connection tracker table to determine if an entry for the flow already exist
2. As flow 3 is not present in the connection tracker table, a lookup is performed in the rule table to identif is applicable to flow 3. The first rule that matches the flow will be enforced.
3. Rule 2 matches for flow 3. The action is set to 'Allow'.
4. Because the action is set to 'Allow' for flow 3, a new entry will be created inside the connection tracker packet is then transmitted out of DFW.

Subsequent packets are processed in this order:

1. A lookup is performed in the connection tracker table to check if an entry for the flow already exists.
2. An entry for flow 3 exists in the connection tracker table. The packet is transmitted out of DFW



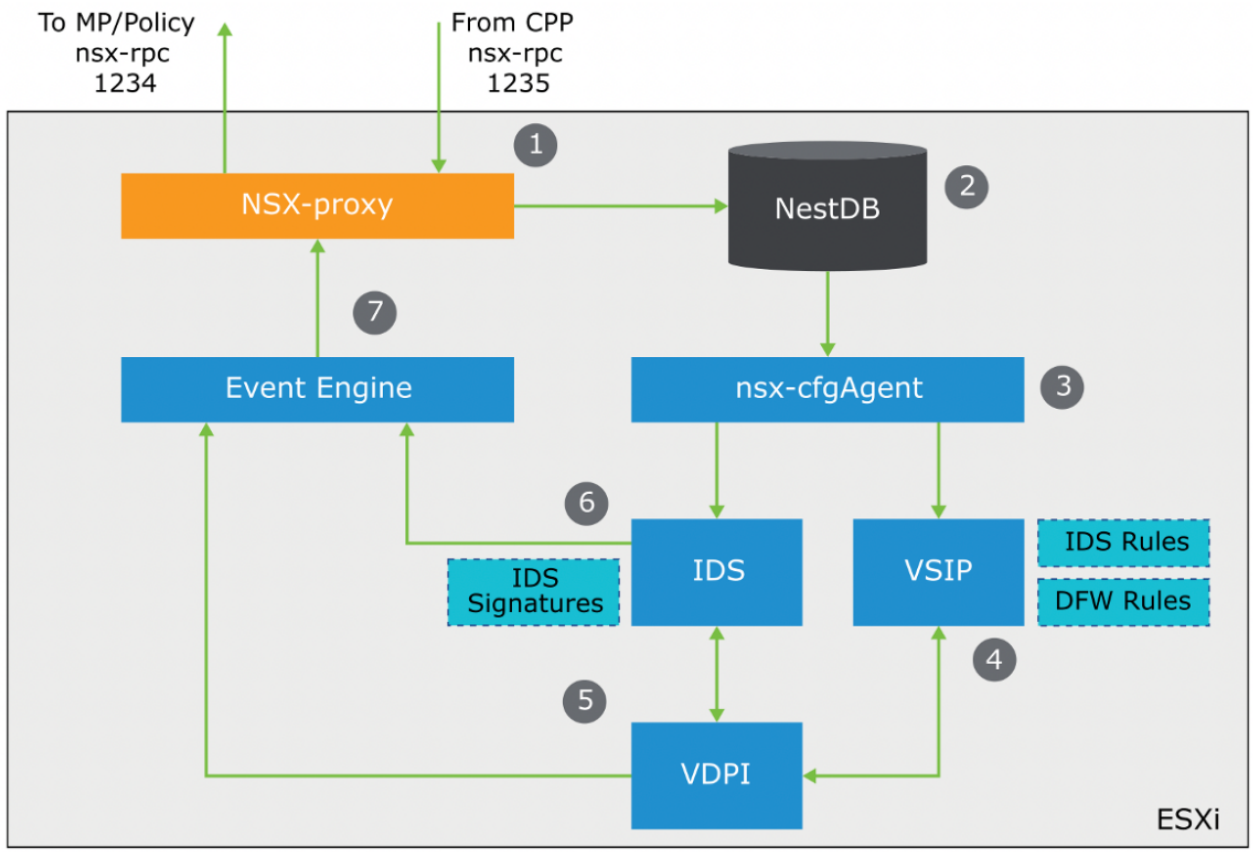
See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-51--rule-lookup

IPS is described further in the Security Reference Guide:

8.1 NSX IPS Components

The NSX IPS components are the same as those described above for DFW as IPS functionality is collocated with DFW. In the Management plane, the Manager downloads IPS signature updates from the cloud service and users configure IPS profiles and rules. As with the DFW, the configuration is passed to the CCP after being stored in the Manager. Again, as with DFW, the CCP pushes the information to the LCP on the hosts. At the host, the signature information is stored in a database on the host and configured in the datapath. The ESXi host also collects traffic data and events to pass up to the NSX manager.

Figure 8 - 2 NSX-T IPS Components – LCP and host below shows the detail of the IPS components inside the host.

	 *See, e.g.*, https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-81-nsx-ips-components
[1e] denying said request if said access request	The Accused Products deny said request if said access request completes a prohibited temporal access pattern for said entity. For example, the VMWare NSX denies said request if said access request completes a prohibited temporal access pattern for said entity.

completes a prohibited temporal access pattern for said entity.	For example, any network traffic requesting access to a computing system is a request in which the NSX determines if it completes a prohibited temporal access pattern. The NSX compares a minimum access level established to a predetermined access level. The request is denied if it does not complete a prohibited temporal access pattern. It does this by employing the Advanced Thread Prevention (ATP) feature. This feature performs Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis. IDS/IPS looks for known malicious traffic patterns which constitute a temporal access pattern. Further, the Network Traffic Analysis uses machine learning and advanced statistical techniques to generate a temporal access pattern. VMware NSX Advanced Threat Prevention At a glance VMware's NSX Advanced Threat Prevention (ATP) provides network security capabilities that protect organizations against advanced threats. NSX ATP combines multiple detection technologies – Intrusion Detection/Prevention System (IDS/IPS), Network Sandboxing, and Network Traffic Analysis (NTA) – with aggregation, correlation, and context engines from Network Detection and Response (NDR). These capabilities complement each other to provide a cohesive defensive layer. As a result, ATP increases detection fidelity, reduces false positives, and accelerates remediation while decreasing security analysts' manual work.

Key capabilities

IDS/IPS

This technology inspects all traffic that enters or leaves the network, detecting and preventing known threats from gaining access to the network, critical systems, and data. IDS/IPS looks for known malicious traffic patterns to hunt for attacks in the traffic flow. When it finds such attacks, it generates alerts for use by security analysts. Alerts are also logged for post-incident investigation.

NTA

This technology looks at network traffic and traffic flow records using machine learning (ML) algorithms and advanced statistical techniques to develop a baseline of everyday activities. NTA can identify protocol, traffic, and host anomalies as they appear. Of course, not all anomalies represent threats; that's why VMware's NTA implements additional ML and rule-based techniques to determine if the anomaly is malicious. This analysis pipeline keeps false positives to a minimum, reducing the security team's work so the team can focus on real issues.

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-advanced-threat-prevention-ds.pdf

Key features	
Context-aware micro-segmentation	Security groups and policies can be dynamically created and automatically updated based on attributes—beyond just IP addresses, ports and protocols—to include elements such as machine name and tags, operating system type and Layer 7 application information to enable adaptive micro-segmentation policy. Policies based on identity information from Active Directory and other sources enable user-level security down to the individual user session level in remote desktop services and virtual desktop infrastructure (VDI) environments.
VMware NSX Intelligence™	Get automated security policy recommendations and continuous monitoring and visualization of every network traffic flow for enhanced visibility, enabling a highly and easily auditable security posture. As part of the same UI as VMware NSX, NSX Intelligence provides a single pane of glass for network and security teams.

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-nsx-gateway-firewall.pdf

For example, this includes malicious IP address filtering, Signature based IDS/IPS and behavior based IDS.

	NSX Distributed Firewall	NSX Distributed Firewall with Threat Prevention	NSX Distributed Firewall with Advanced Threat Prevention
L2 – L4 firewalling	X	X	X
L7 Application Identity based firewalling	X	X	X
User Identity based firewalling	X	X	X
NSX Intelligence (flow visualization, policy recommendation)	X	X	X
Malicious IP address filtering	X	X	X
vRealize Log Insight	X	X	X
Signature based IDS/IPS		X	X
Behavior based IDS		X	X
NTA			X
Network Sandbox			X
NDR			X

See, e.g., https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-nsx-distributed-firewall.pdf

	This is further described in the NSX Reference Design Guide:

5 NSX Security

In addition to providing network virtualization, NSX also serves as an advanced security platform, providing a rich set of features to streamline the deployment of security solutions. This chapter focuses on core NSX security capabilities, architecture, components, and implementation. Key concepts for examination include:

- NSX distributed firewall (DFW) provides stateful protection of the workload at the vNIC level. For ESXi, the DFW enforcement occurs in the hypervisor kernel, helping deliver micro-segmentation. However, the DFW extends to physical servers, KVM hypervisors, containers, and public clouds providing distributed policy enforcement.
- Uniform security policy model for on-premises and cloud deployment, supporting multi-hypervisor (i.e., ESXi and KVM) and multi-workload, with a level of granularity down to VM/containers/bare metal attributes.
- Agnostic to compute domain - supporting hypervisors managed by different compute-managers while allowing any defined micro-segmentation policy to be applied across hypervisors spanning multiple vCenter environments.
- Support for Layer 3, Layer 4, Layer-7 APP-ID, & Identity based firewall policies provide security via protocol, port, and or deeper packet/session intelligence to suit diverse needs.
- NSX Gateway firewall serves as a centralized stateful firewall service for N-S traffic. Gateway firewall is implemented per gateway and supported at both Tier-0 and Tier-1. Gateway firewall is independent of NSX DFW from policy configuration and enforcement perspective, providing a means for defining perimeter security control in addition to distributed security control.
- Gateway & Distributed Firewall Service insertion capability to integrate existing security investments using integration with partner ecosystem products on a granular basis without the need for interrupting natural traffic flows.
- Distributed IDS extends IDS capabilities to every host in the environment.
- Dynamic grouping of objects into logical constructs called Groups based on various criteria including tag, virtual machine name or operating system, subnet, and segments which automates policy application.
- The scope of policy enforcement can be selective, with application or workload-level granularity.
- Firewall Flood Protection capability to protect the workload & hypervisor resources.
- IP discovery mechanism dynamically identifies workload addressing.
- SpoofGuard blocks IP spoofing at vNIC level.

- Switch Security provides storm control and security against unauthorized traffic.

NSX 3.2 introduces advanced security features such as security on vCenter dvpgs, distributed and centralized malware protection, centralized IDS/IPS, URL Filtering, extensive next generation firewall App Identification support, Network Traffic Anomaly Detection, and Network Detection and Response (NDR). These new features will be covered in the new version if the SECURITY DESIGN GUIDE. This document will cover the NSX core security feature.

5.5 Intrusion Detection

Much like distributed firewalling changed the game on firewalling by providing a distributed, ubiquitous enforcement plane, NSX distributed IPS/IPS changes the game on IPS by providing a distributed, ubiquitous enforcement plane. However, there are additional benefits that the NSX distributed IPS model brings beyond ubiquity (which in itself is a game changer). NSX IPS is IPS distributed across all the hosts. Much like with DFW, the distributed nature allows the IPS

	capacity to grow linearly with compute capacity. Beyond that, however, there is an added benefit to distributing IPS. This is the added context. Legacy network Intrusion Detection and Prevention systems are deployed centrally in the network and rely either on traffic to be hairpinned through them or a copy of the traffic to be sent to them via techniques like SPAN or TAPs. These sensors typically match all traffic against all or a broad set of signatures and have very little context about the assets they are protecting. Applying all signatures to all traffic is very inefficient, as IDS/IPS unlike firewalling needs to look at the packet payload, not just the network headers. Each signature that needs to be matched against the traffic adds inspection overhead and potential latency introduced. Also, because legacy network IDS/IPS appliances just see packets without having context about the protected workloads, it's very difficult for security teams to determine the appropriate priority for each incident. Obviously, a successful intrusion against a vulnerable database server in production which holds mission-critical data needs more attention than someone in the IT staff triggering an IDS event by running a vulnerability scan. Because the NSX distributed IDS/IPS is applied to the vNIC of every workload, traffic does not need to hairpinned to a centralized appliance, and we can be very selective as to what signatures are applied. Signatures related to a windows vulnerability don't need to be applied to Linux workloads, or servers running Apache don't need signatures that detect an exploit of a database service. Through the Guest Introspection Framework, and in-guest drivers, NSX has access to context about each guest, including the operating system version, users logged in or any running process. This context can be leveraged to selectively apply only the relevant signatures, not only reducing the processing impact, but more importantly reducing the noise and quantity of false positives compared to what would be seen if all signatures are applied to all traffic with a traditional appliance. For a detailed description of IDS configuration, see the NSX Product Documentation.

5.7 Additional Security Features

NSX extends the security solution beyond DFW with additional features to enhance data center security posture on top of micro-segmentation. These features include:

- **SpoofGuard** - Provides protection against spoofing with MAC+IP+VLAN bindings. This can be enforced at a per logical port level. The SpoofGuard feature requires static or dynamic bindings (e.g., DHCP/ARP snooping) of IP+MAC for enforcement.
- **Segment Security** - Provides stateless L2 and L3 security to protect segment integrity by filtering out malicious attacks (e.g., denial of service using broadcast/multicast storms) and unauthorized traffic entering segment from VMs. This is accomplished by attaching the segment security profile to a segment for enforcement. The segment security profile has options to allow/block bridge protocol data unit (BPDU), DHCP server/client traffic, non-IP traffic. It allows for rate limiting of broadcast and multicast traffic, both transmitted and received.

See, e.g., https://communities.vmware.com/t5/VMware-NSX-Documents/VMware-NSX-T-Reference-Design/ta-p/2778093

Virtual Firewalling is described further in the Security Reference Guide:

5.1 Rule Lookup

NSX firewalls implement a top down rule search order. When a packet matches, it pops out of the search bas processing indicated in the matched rule.

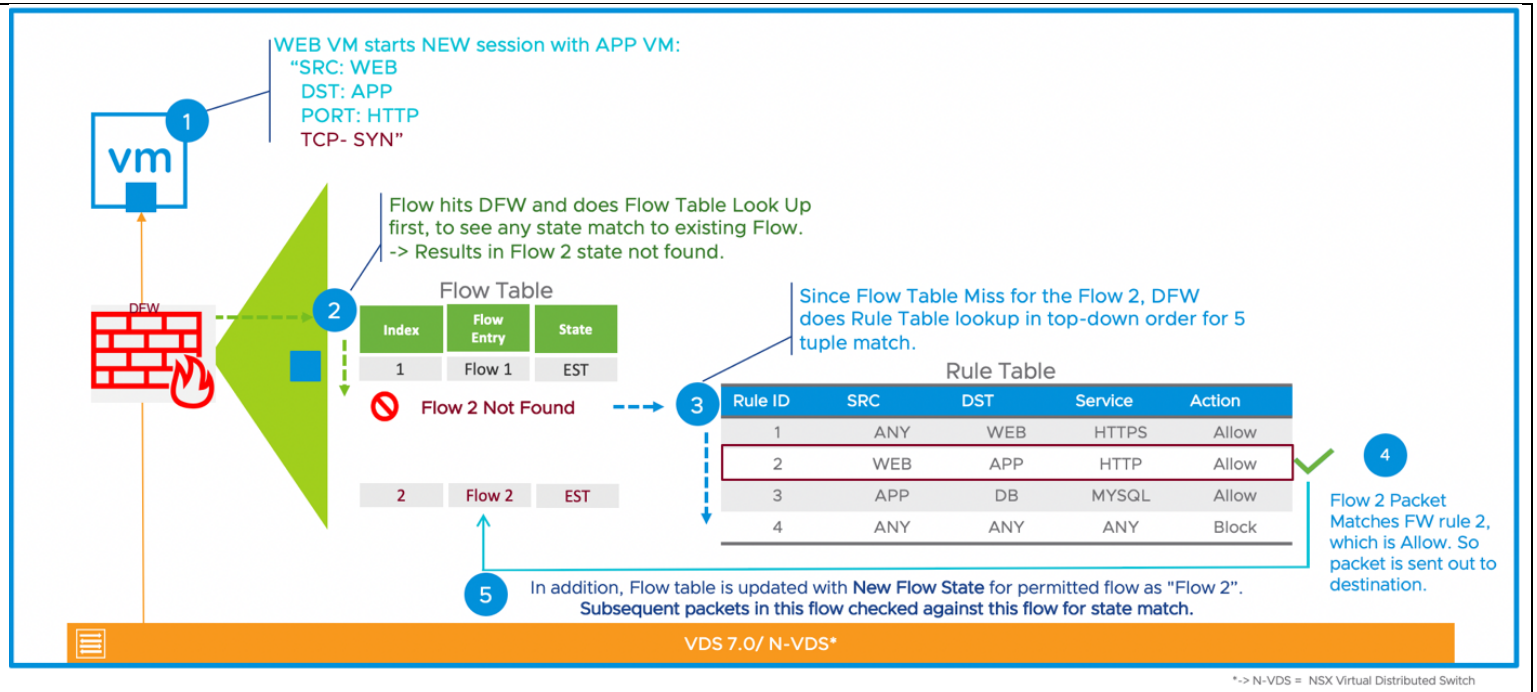
By default, the DFW implements the rule table and flow table model that most firewalls use. However, this bel overwritten for troubleshooting or other corner cases as described later.

In figure 4.1, the processing of a packet takes place as follows:
An IP packet identified as pkt1 that matches rule number 2. The order of operation is the following:

1. A lookup is performed in the connection tracker table to determine if an entry for the flow already exist
2. As flow 3 is not present in the connection tracker table, a lookup is performed in the rule table to identif is applicable to flow 3. The first rule that matches the flow will be enforced.
3. Rule 2 matches for flow 3. The action is set to 'Allow'.
4. Because the action is set to 'Allow' for flow 3, a new entry will be created inside the connection tracker packet is then transmitted out of DFW.

Subsequent packets are processed in this order:

1. A lookup is performed in the connection tracker table to check if an entry for the flow already exists.
2. An entry for flow 3 exists in the connection tracker table. The packet is transmitted out of DFW



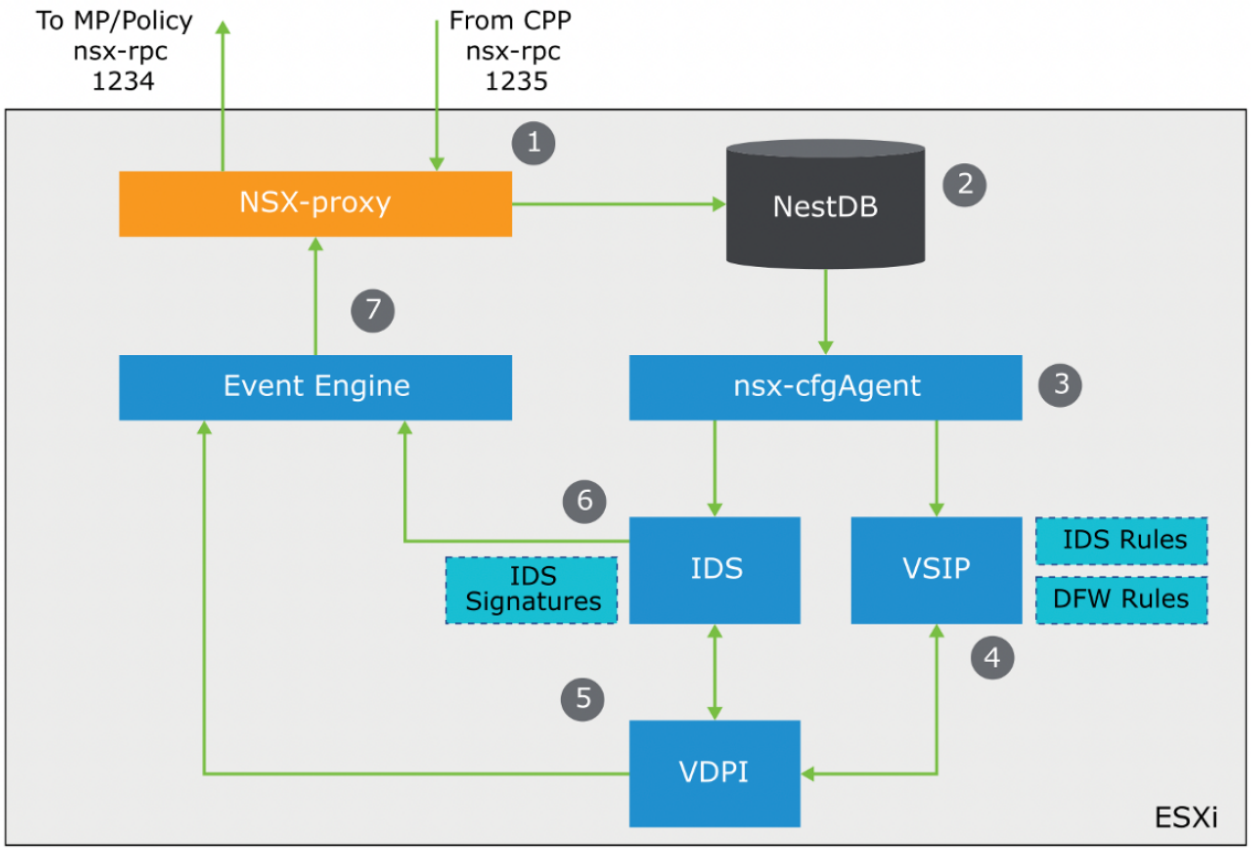
See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-51--rule-lookup

IPS is described further in the Security Reference Guide:

8.1 NSX IPS Components

The NSX IPS components are the same as those described above for DFW as IPS functionality is collocated with DFW. In the Management plane, the Manager downloads IPS signature updates from the cloud service and users configure IPS profiles and rules. As with the DFW, the configuration is passed to the CCP after being stored in the Manager. Again, as with DFW, the CCP pushes the information to the LCP on the hosts. At the host, the signature information is stored in a database on the host and configured in the datapath. The ESXi host also collects traffic data and events to pass up to the NSX manager.

Figure 8 - 2 NSX-T IPS Components – LCP and host below shows the detail of the IPS components inside the host.



See, e.g., https://nsx.techzone.vmware.com/resource/nsx-security-reference-design-guide#a-81-nsx-ips-components